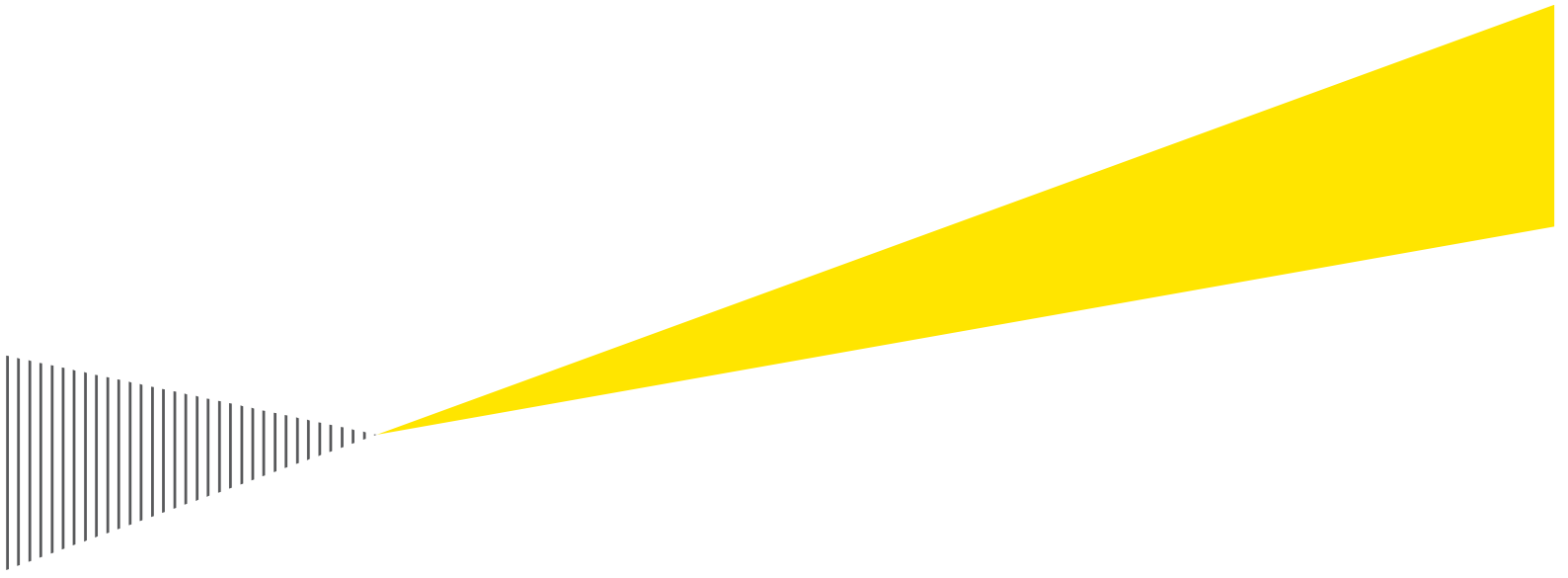
Revisionsrapport 2019
Genomförd på uppdrag av revisorerna
Maj 2019

Kävlinge kommun

Granskning av behörighet till känsliga uppgifter samt interna kontroller



Building a better working world

Innehåll

1. Sammanfattning

EY har på uppdrag av kommunrevisionen i Kävlinge granskat omsorgsnämndens och kommunstyrelsens arbete med behörigheter, åtkomst och loggkontroller. Kommunstyrelsen har granskats utifrån sitt lednings- och samordningsansvar och inom omsorgsnämndens ansvarsområde har granskningen omfattat arbetet inom två verksamhetssystem.

Vår sammanfattande bedömning är att arbetet med behörigheter, åtkomster och loggkontroller inte fungerar helt ändamålsenligt, därtill bedömer vi att den interna kontrollen inte är fullt ut tillräcklig. Vi bedömer att kommunstyrelsens övergripande styrning inom området bör stärkas och att styrelsen bör förtydliga riktlinjer och rekommendationer kring systemförvaltningen och säkerställa att verksamheterna upprättar adekvat systemdokumentation.

Avseende omsorgsnämnden är det vår bedömning att arbetet med behörigheter, åtkomster och loggkontroller inte fungerar helt ändamålsenligt. Vi bedömer att nämnden behöver stärka styrningen av behörigheter och även stärka den interna kontrollen.

Vi har bland annat gjort följande iakttagelser:

- Kommunfullmäktige har antagit en informationssäkerhetspolicy. I skrivande stund pågår arbetet med att ta fram tillhörande strategi och riktlinjer.
- Kommunerna som ingår i samarbetsnämnden har en gemensam systemförvaltningsmodell som fastställer ansvar och rollfördelning för specifika IT-system. Det finns även en mall för systemförvaltningsplaner.
- Det saknas systemförvaltningsplaner för de granskade verksamhetssystemen.
- Det finns rutiner för behörighetstilldelning för båda verksamhetssystemen. Dock saknas dokumenterade förteckningar över och villkor för behörighetstilldelning.
- I Procapita VOO finns i dagsläget 33 behörighetsgrupper. 16 av dessa grupper, ca 400 användare, har kommunövergripande läsbehörighet. Samtliga 16 enhetschefer har behörighet att nå samtliga brukare i systemet, detta för att kunna täcka upp för varandra vid frånvaro.
- Det finns rutiner för åtkomstkontroll (loggkontroller) för de granskade verksamhetssystemen.
- En del personalgrupper som använder Procapita omfattas inte av loggkontrollerna, så som enhetschefer, systemförvaltare och MAS. Därtill omfattas inte heller personal som har begränsad behörighet, såsom personal som arbetar på gruppbostäder eller särskilt boende. Detta innebär i praktiken att ca 400 användare inte omfattas av genomförda loggkontroller.
- Det sker ingen uppföljning eller kontroll av att granskningsprotokoll från åtkomstkontrollerna inkommer.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Stärka styrningen av arbetet med informationssäkerhet i kommunens verksamhetssystem.

Utifrån granskningsresultatet rekommenderar vi omsorgsnämnden att:

- Stärka styrningen vid behörighetstilldelning.
- Säkerställa att åtkomstkontroller sker i den utsträckning som krävs i fråga om frekvens och omfattning.
- Upprätta systemförvaltarplaner i enlighet med systemförvaltarmodellen.

2. Inledning

2.1. Bakgrund

Behörigheter till kommunens verksamhetssystem som innehåller känsliga persondata regleras av olika lagar såsom dataskyddsförordningen. Det ska finnas en rättslig grund för de uppgifter som kommunen registrerar om personer. Uppgifterna ska också skyddas så att ingen obehörig kan få del av uppgifterna.

Omsorgsnämndens verksamheter har med åren blivit alltmer beroende av IT-stöd, vilket innebär nya former av hot och risker. Behörighetsstyrning och interna kontroller är en viktig del i arbetet för att skydda uppgifterna och möta lagkrav. I detta ligger att upprätta och upprätthålla rättigheter för användare i de IT-system som brukas, så att användarna enbart får och har åtkomst till den information som behövs i det dagliga arbetet. En bristfällig styrning och kontroll inom området kan riskera att verksamheten inte bedrivs på ett ändamålsenligt sätt samt att känslig information sprids till icke behöriga.

De förtroendevalda revisorerna har med utgångspunkt i ovanstående beslutat genomföra en granskning avseende hanteringen av behörigheter i relation till känsliga persondata. Granskningen avser omsorgsnämnden och kommunstyrelsen.

2.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om nämndens och styrelsens arbete med behörigheter, åtkomster och loggkontroll i verksamhetssystemen hanteras på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

I granskningen besvaras följande revisionsfrågor:

- Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?
- Är uppföljning och utvärdering inom området ändamålsenlig?
- Sker en tillräcklig styrning av behörigheter till känsliga system?
- Säkerställer nämnderna att tillräcklig intern kontroll inom området har upprättats för att hindra otillåten åtkomst till och spridning av känslig information?

2.3. Genomförande och avgränsning

Granskningen inom omsorgsnämndens ansvarsområde omfattar två verksamhetssystem. Följande verksamhetssystem omfattas av granskningen:

- Procapita vård- och omsorg
- Nationell Patient Översikt (NPÖ)

Granskningen sker genom intervjuer med ansvariga tjänstemän och dokumentstudier. Verifiering av den interna kontrollen sker genom loggkontroller i de granskade systemen och avstämning mot vilka funktioner som har skäl att ta del av informationen.

Kommunstyrelsen granskas utifrån sitt lednings- och samordningsansvar.

2.4. Revisionskriterier

2.4.1. Kommunallagen (2017:725) kap 6

Kommunallagens 6 kap redogör för kommunstyrelsens och nämndernas uppgifter. 1§ fastställer att kommunstyrelsen ska leda och samordna kommunens angelägenheter och ha uppsikt över övriga nämnder.

Nämnderna ska enligt 6§ inom sitt ansvarsområde se till att verksamheten bedrivs i enlighet med kommunfullmäktiges mål och riktlinjer. Därtill ska nämnderna se till att den interna kontrollen är tillräcklig.

2.4.2. Patientdatalagen (2008:355)

Patientdatalagen reglerar behandling av personuppgifter inom hälso- och sjukvården. I lagens 4 kap framgår grundläggande bestämmelser om inre sekretess och elektronisk åtkomst. Inre sekretess innebär att den som arbetar hos en vårdgivare (kommunen) endast får ta del av en patients dokumenterade uppgifter om denne deltar i vård av patienten, eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

Av 4 kap 2§ framgår att vårdgivaren ska bestämma villkor för tilldelning av behörighet för åtkomst till patienters uppgifter, denna behörigheten ska begränsas till det som krävs för den anställde att fullgöra sina arbetsuppgifter. Enligt 3§ ska vårdgivaren göra systematiska och återkommande kontroller av åtkomst till patienters uppgifter. Dessa bestämmelser gäller även för sammanhållen journalföring. För sammanhållen journalföring krävs även patientens samtycke.

Datainspektionen har tagit fram en vägledning för hälso- och sjukvården utifrån patientdatalagens bestämmelser. I vägledningen framgår att vårdgivare bör göra en risk- och väsentlighetsanalys inför beslut om behörighetstilldelning, för att säkerställa en väl avvägd behörighetstilldelning. Datainspektionen understryker att vårdgivaren i detta fall har ett ansvar att säkerställa att analysen faktiskt genomförs och dokumenteras.

Därtill menar Datainspektionen att det bör finnas riktlinjer för den personal som genomför kontroller av loggar. Riktlinjerna ska stötta denna personal och tydliggöra vad som utgör obehörig elektronisk åtkomst och möjliggöra att det finns gemensamma utgångspunkter för detta.

2.4.3. Socialstyrelsens föreskrifter om allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

Socialstyrelsen har tagit fram föreskrifter med stöd av patientsäkerhetsförordningen och patientdataförordningen. Föreskrifterna är framtagna med stöd av Datainspektionen. I 3 kap. 4§ (HSLF-FS 2016:40) anges att vårdgivaren ska ansvara för att det finns en informationssäkerhetspolicy som anger övergripande mål och inriktning på verksamhetens arbete med informationssäkerhet.

Vårdgivaren ska utse en eller flera personer som leder och samordnar informationssäkerhetsarbetet. Denne ska årligen sammanställa:

- Riskanalyser kopplat till informationssäkerhetsarbetet
- Incidenter som påverkat informationssäkerhetsarbetet
- Uppföljningar
- Förbättringsåtgärder

Enligt 4 kap 2-3§§ ska vårdgivaren ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter, detta beslut ska föregås av en behovs- och riskanalys (se även 2.4.2). Det ska även finnas rutiner för ändring, borttag och regelbunden uppföljning för att säkerställa att behörigheterna är riktiga och aktuella.

4 kap 9§ berör kontroll av åtkomst till personuppgifter. I föreskrifterna framgår att det ska genomföras systematiska och återkommande stickprovskontroller av loggar, att dessa kontroller dokumenteras och att loggarna sparas i minst 5 år.

Vårdgivaren ska även enligt 3 kap 5§ förlöpande bedöma om det finns risker i verksamheten som kan medföra att kraven i föreskrifterna inte uppfylls, sådana riskanalyser ska dokumenteras.

2.4.4. Dataskyddsförordningen (GDPR)

Den 25 maj 2018 trädde dataskyddsförordningen (GDPR) i kraft och ersatte personuppgiftslagen (PUL). Förordningen innebär stärkta rättigheter och skydd för individen vad gäller information och samtycke samt ett ökat ansvar för personuppgiftsansvariga. Ett sätt att säkerställa att personuppgiftsbehandlingen är i överensstämmelse med lagstiftningen kan vara att anta uppförandekoder, interna riktlinjer och förfaranden.

3. Granskningsresultat

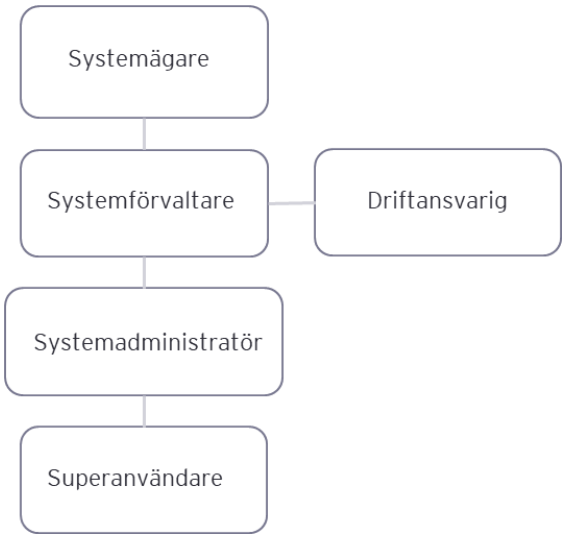
3.1. Övergripande organisation och styrning

Kommunstyrelsen har enligt sitt reglemente hand om kommunens IT-system, som en del i dess lednings- och styrfunktion. Därutöver ingår Kävlinge kommun tillsammans med Burlövs och Staffanstorps kommuner i en samarbetsnämnd som utgör en gemensam IT-driftsorganisation. Den gemensamma IT-organisationen benämns IT-teamet och dess huvuduppgift är att ansvara för drift och utveckling av kommunernas samlade IT-plattform, infrastrukturen knuten till IT-tjänster, stödja verksamhetsutveckling och samarbeta kring IT-säkerhet. Kävlinge kommun fungerar som beställarfunktion och har en utsedd IT-strateg (motsvarande IT- chef).

3.1.1. Systemförvaltarmodell

Kommunerna som ingår i samarbetsnämnden har en gemensam systemförvaltningsmodell som fastställer ansvar och rollfördelning för specifika IT-system. I modellen anges att kommunstyrelsen har ett övergripande ansvar för IT-systemen inom respektive kommun. Respektive nämnd är ansvarig för de IT-system som används inom dess verksamhetsområde.

För varje IT-system är följande roller obligatoriska att tillsätta: systemägare, systemförvaltare samt driftansvarig. I nedanstående bild framgår samtliga roller som kan ingå i systemförvaltningsorganisationen.



Graf: Rollfördelning systemförvaltarmodell.

Systemägaren har det övergripande ansvaret för att förvaltning av systemet fungerar, att rutiner finns framtagna samt att såväl personella som ekonomiska resurser finns tillgängliga. Utöver detta ingår ett antal uppgifter så som att upprätthålla rutiner för informationssäkerhet, tillse att systemförvaltaren har rätt kompetens och att säkerställa att erforderliga avtal finns. Systemägaren godkänner även systemförvaltningsplanen.

Systemförvaltaren ansvarar genom delegation från systemägaren för den dagliga användningen av systemet. Det är framförallt denna roll som handhar administration kring systemet, tar fram systemförvaltningsplan och säkerställer att denna följs. Som systemförvaltare arbetar man även med support och information till användare och upprättar systemdokumentation.

Driftansvarig är en person utsedd av IT-teamet och ska säkerställa att den tekniska förvaltningen sker enligt driftsavtal (SLA). Den driftansvariga är systemförvaltarens kontaktperson på IT-teamet. Driften består i systemuppgraderingar, övervakning av systemet (felsökning) och upprätta/hålla dokumentation kring driftsrutiner.

Systemadministratör fungerar som en stödfunktion till systemförvaltaren och utses vid behov. Bistår med behörighetsadministration, supportärende och utbildningar.

Superanvändare är personer ute i verksamheterna som har fördjupad kunskap om systemet. Dessa personer kan ge utökad support till andra användare.

Utöver rollbeskrivningen listas även den systemdokumentation som ska finnas för varje system, listan ska ses som ett minimumkrav:

- Systembeskrivning (leverantör bistår vanligtvis med detta)
- Avtal med leverantör
- Personuppgiftbiträdesavtal vid extern drift
- Systemförvaltningsplan
- Driftsavtal och SLA-bilaga

Det finns en framtagen mall för systemförvaltningsplan, denna innehåller information om roller och ett avsnitt om planerade aktiviteter för det specifika systemet. Det finns forum på olika nivåer som behandlar frågor kring IT-systemen. Dessa beskrivs i systemförvaltarmodellen (se sammanställning i bilaga 2), dock är endast avtalsuppföljningen obligatorisk. Vid intervju uppges att dessa forum i praktiken består av sammansatta grupper som kommunicerar via kommunens intranät. Exempelvis finns en grupp där samtliga systemförvaltare ingår och har möjlighet att diskutera frågeställningar och gemensamma utmaningar. Det finns även möjlighet att skapa grupper utifrån behov. Detta uppges fungera bra och är ett flexibelt sätt för olika funktioner att mötas.

3.1.2. Styrdokumentation

I likhet med systemförvaltarmodellen finns en gemensam IT-policy som gäller för kommunerna som ingår i samarbetsnämnden. IT-policyn togs fram 2013 och har antagits av kommunfullmäktige i Kävlinge. Kopplat till policyn finns en IT-strategi som beskriver hur den gemensamma IT-plattformen ska underhållas och utvecklas.

I Kävlinge kommun finns även en informationssäkerhetspolicy och strategi för hantering av allmänna dataskyddsförordningen. Dessa styrdokument är framtagna av Kävlinge kommun och omfattas inte av samarbetsnämnden. Strategi för hantering av allmänna dataskyddsförordningen antogs av kommunstyrelsen 2018-04-25. Strategin beskriver på en övergripande nivå de krav som åläggs kommunens verksamheter i samband med lagens ikraftträdande. Det anges bland annat att varje nämnd ska upprätta egna riktlinjer för hantering av allmänna dataskyddsförordningen. Omsorgsnämnden har ingen sådan riktlinje utan hänvisar till den kommunövergripande strategin och de rutiner som säkerhetsenheten tagit fram inför införandet av GDPR. Det pågår i skrivande stund ett arbete med att ta fram informationsstrategi och riktlinjer för informationssäkerhet som även ska omfatta riktlinjer för hantering av allmänna dataskyddsförordningen. Informationssäkerhetsstrategin planeras att tas upp för beslut under hösten 2019 och riktlinjerna senast under 2020.

Varje nämnd ska även utse minst en informationssäkerhetssamordnare som får i uppgift att säkerställa att dataskyddsförordning och kommunens styrdokument inom området efterlevs. Denna funktion ska verka stödjande gentemot anställda inom verksamheten. Inom omsorgsnämnden är systemförvaltare för Procapita VOO och NPÖ även informationssäkerhetssamordnare.

3.1.3. Bedömning

Vi bedömer att styrning och ledning inom området i stort är ändamålsenlig. Vi kan dock se ett behov av att revidera systemförvaltarmodellen så att den överensstämmer med hur arbetet ser ut i praktiken, så som avseende forumen. Därtill bedömer vi att även mallen för systemförvaltningsplan kan behöva ses över i syfte att möjliggöra en tydligare styrning av verksamhetssystemen. I detta avseende menar vi att systemförvaltningsplanen kan fungera som en utgångspunkt där rutiner och aktiviteter kring ett specifikt objekt samlas.

Vidare bedömer vi att kommunstyrelsen har anledning att ytterligare förtydliga vilka övergripande krav som finns avseende behörighetsstyrning, gallring och loggkontroller i syfte att säkerställa att verksamheterna beaktar detta i sin systemförvaltning.

3.2. Procapita Vård och Omsorg

Procapita är det huvudsakliga verksamhetssystemet som används inom sektor omsorg. I princip all information som lagras i systemet bedöms vara känslig information. Detta omfattar allt från utredningar och utförandedokumentation enligt socialtjänstlagen, LSS och färdtjänst till hälso- och sjukvårdsjournaler.

Procapita VOO har en systemförvaltare som även fungerar som informationssäkerhetssamordnare för sektor omsorg. Systemförvaltaren är organisatoriskt placerad under kommunikationsenheten, som är en del av verksamhetsstöd. Ansvarig chef för systemförvaltaren är kommunikationschefen. Utöver systemförvaltaren finns driftansvariga tekniker som ligger under IT-teamet. Systemägare för Procapita VOO är sektorschef för omsorg. Det finns två assistenter som arbetar med Procapita VOO, dessa bistår systemförvaltaren med behörighetsadministration och lösenordshantering. Assistenterna tillhör kanslienheten, som också är en del av verksamhetsstöd. Vid tiden för granskningen fanns 984 användare i systemet, fördelade på 33 behörighetsgrupper (se även avsnitt 3.2.1)

Enligt uppgift finns en IT-grupp för hälso- och sjukvård där legitimerad personal, MAS (medicinskt ansvarig sjuksköterska) och IT-samordnare (tillika systemförvaltare) är representerande, som träffas 3-4 gånger om året. Fokus för gruppens träffar har varit dokumentation och information i hälso- och sjukvårdsjournalen i Procapita. Enligt 2018 års patientsäkerhetsberättelse genomfördes en riskanalys i enlighet med Socialstyrelsens föreskrift (HSLF-FS 2016:40) 3 kap 5§.

Det saknas en dokumenterad systemförvaltningsplan för systemet. De intervjuade uppger att utveckling och underhåll av systemet sker löpande under året i samråd med verksamhet och driftansvariga tekniker. Detta sker bland annat enligt en upprättad rutin som beskriver arbetsfördelning vid servicefönster (uppdateringar och underhåll av systemet).

3.2.1. Behörigheter

Enligt upprättad rutin ska ansvarig chef (verksamhetschef eller enhetschef) besluta om vilken behörighet en anställd ska ha. Beställningen skickas till systemförvaltaren genom ett formulär på kommunens intranät och innehåller följande:

- Namn
- Personnummer
- Användarnamn
- Arbetsplats/enhet
- Roll

Systemförvaltare eller assistent lägger sedan upp användaren i Procapita enligt beställning. Ansvarig chef har därutöver ansvar för att meddela systemförvaltare eller assistent om en medarbetare avslutar sin anställning, byter arbetsplats eller i det fall medarbetaren kommer vara frånvarande under en längre tid. Vid intervju uppges att rutinen i de flesta fall fungerar, men också att chefer missar att meddela förändringar som påverkar behörigheten. För att kunna nå Procapita måste personalen vara inne på Kävlinge kommuns nätverk.

De olika behörighetsgrupperna är primärt indelade efter yrkesroller och detta styr vad man som användare kan göra i systemet. Därefter får de olika grupperna tilldelade dataurval, som styr vilka delar som en användare har tillgång att se i systemet. På så sätt kan användarens behörighet anpassas efter yrkesroll och arbetsplats. Det saknas en dokumenterad förteckning över vilka yrkesgrupper som ska tilldelas specifika grupper och dataurval. Det finns dock inlagt i systemets behörighetstilldelningsfunktion vilka grupper och dataurval som är tillgängliga.

I Procapita VOO finns i dagsläget 33 behörighetsgrupper. 16 av dessa grupper, ca 400 användare, har kommunövergripande läsbehörighet. De yrkesgrupperna med bredast behörighet är legitimerad personal, enhetschefer, nattpersonal, biståndshandläggare och resurspersonal från bemanningsenheten. Vid intervju uppges att resurspersonalen kommer att få en mer begränsad behörighet framöver, då man håller på att se över fördelningen av deras arbetsuppgifter. Vidare uppges att samtliga enhetschefer har behörighet att nå samtliga brukare i systemet, detta för att kunna täcka upp för varandra vid frånvaro. För närvarande finns 16 enhetschefer inom sektor omsorg.

Enligt styrdokumentet informationssäkerhet Procapita VOO ska gallring av behörigheter ske minst en gång per år, respektive enhetschef ansvarar för detta. Dock framgår av rutinen för åtkomstkontroll (se avsnitt 3.2.2) att antal behöriga per behörighetsgrupp ska kontrolleras en gång i kvartalet. Systemförvaltaren skickar ut en förteckning över användare kopplade till specifika enheter, varpå enhetschef kontrollerar att detta överensstämmer med antal personal, behov och funktioner. Vid intervju framgick även att det vid årsskiftet genomfördes en större gallring som innebar att användare som lades upp under 90-talet togs bort. Resultat av genomförda gallringar dokumenteras inte.

3.2.2. Loggkontroller

I styrdokumentet informationssäkerhet Procapita VOO framgår att åtkomstkontroll i form av loggkontroller ska genomföras en gång i kvartalet. Rutinen för loggkontrollen är även dokumenterad i två separata styrdokument framtagna av systemförvaltaren och MAS. Rutinen berör loggkontroller för vårdpersonal respektive legitimerad personal:

Vårdpersonal: En gång per kvartal tas loggar fram av läs- och skrivaktivitet under en månads tid. Urvalet baseras per behörighetsgrupperna i systemet, där ett slumpmässigt urval görs av personal i varje grupp. Målet är att varje vårdpersonal ska granskas minst en gång om året. Loggarna skickas sedan till ansvarig enhetschef som ska kontrollera loggarna utifrån vård- och omsorgsrelation. Chefen ska fylla i ett granskningsprotokoll där det framgår vilken personal som har granskats, hur många aktiviteter som funnits under perioden och markera eventuella anmärkningar. Det finns även möjlighet för enhetschef att kommentera eventuella åtgärder som vidtagits med anledning av kontrollen. Protokollet skickas sedan manuellt in till systemförvaltaren som sparas dessa i en pärm.

Legitimerad personal: En gång per kvartal kontrolleras även legitimerad personal (sjuksköterskor, arbetsterapeuter och sjukgymnaster). Urvalet av loggarna begränsas till en hel dag, där ansvarig chef ska granska vilken personal som läst vad i patienternas journaler. I likhet med ovanstående ska ett granskningsprotokoll fyllas i av ansvarig chef som sedan sparas i systemförvaltarens pärm.

Vid intervju framkom att det även genomförs riktade loggkontroller avseende kända personer, vid familjerelation eller vid misstanke. Det finns även en upprättad rutin för misstanke om dataintrång som beskriver hur handläggning och eventuella åtgärder ska hanteras. Vidare framkommer att en del personalgrupper inte omfattas av loggkontrollerna, så som enhetschefer, systemförvaltare och MAS. Därtill omfattas inte heller personal som har begränsad behörighet, såsom personal som arbetar på gruppbostäder eller särskilt boende. Detta innebär i praktiken att ca 400 användare inte omfattas av genomförda loggkontroller.

Det genomförs ingen uppföljning av att samtliga granskningsprotokoll har inkommit till systemförvaltaren i samband med loggkontroller. På grund av tidsbrist uppger de intervjuade att loggkontrollerna genomförts en gång per halvår och inte en gång per kvartal som framgår av riktlinjerna.

3.2.3. Bedömning

Vår bedömning är att styrning, kontroll och uppföljning i vissa delar sker ändamålsenligt. Granskningen visar att det finns dokumenterade rutiner men också att dessa inte följs i full utsträckning, därtill bedömer vi att dokumentationen inom vissa områden bör utökas och förtydligas. I fråga om styrning av behörigheter bedömer vi att med bakgrund av skrivningar i patientdatalagen och i Datainspektionens rekommendationer att behörighetstilldelningen bör ses över. Vi bedömer att detta särskilt bör beaktas för yrkesgrupper som idag har mycket bred behörighet, så som enhetschefer. Därtill bedömer vi att avsaknaden av dokumenterade villkor för behörighetstilldelning bör åtgärdas.

Vi bedömer att nuvarande rutiner för loggkontroller med fördel kan utökas med riktlinjer för dem som utför kontrollen, så som framgår av Datainspektionens rekommendationer. Utöver detta bedömer vi att uppföljningen av granskningsprotokollen inte fungerar ändamålsenligt. I detta avseende bör omsorgsnämnden stärka den interna kontrollen. Granskningen visar bland annat att kontrollerna inte genomförs med den frekvens som framgår av fastställda riktlinjer vilket föranleder att nämnden bör säkerställa att det finns möjlighet för ansvariga att genomföra kontrollerna. Vidare bedömer vi att den loggkontroll som genomförs idag är otillräcklig då den inte omfattar samtlig personal, återigen särskilt med beaktande av att enhetschefer har mycket bred behörighet.

Slutligen bedömer vi att det är en brist att det saknas en dokumenterad systemförvaltningsplan för Procapita VOO. Vi bedömer att en sådan plan kan bidra till att samla information och dokumentation om systemet vilket möjliggör transparens och tillgänglighet. Vid avsaknaden av en plan med fastställda aktiviteter finns en risk att personberoende skapas och att åtgärder sker ad hoc. Utöver detta bedömer vi att en väl utformad systemförvaltningsplan bidrar till att illustrera omfattning av åtgärder, underhåll och kontroller vilket ger underlag för en avvägd planering.

3.3. Nationell patientöversikt

Nationell patientöversikt (NPÖ) är ett system för sammanhållen journalföring, där olika vårdgivare kan dela information från patienters journaler. I Kävlinge kommun används systemet för att legitimerad personal ska kunna ta del av journalanteckningar avseende brukare som har vårdats inom framförallt Region Skånes regi.

För att personal ska få tillgång till journaluppgifterna i NPÖ måste brukaren ge sitt samtycke. Vid varje ny vårdrelation ska personalen informera om NPÖ och sedan dokumentera i Procapita VOO att brukaren har gett sitt samtycke. För detta finns en upprättad rutin som även beskriver hur man ska gå tillväga om samtycke inte kan inhämtas.

MAS träffas tillsammans med IT-samordnare löpande under året, ca 3-4 gånger per termin och diskuterar användning, utbildning och verksamhetsutveckling med hjälp av systemet. Det saknas en systemförvaltningsplan för NPÖ, vilket vid sakkontroll uppges vara på grund av att systemet ägs av INERA som bistår regioner och kommuner med digitala tjänster.

3.3.1. Behörigheter

Som nämnts ovan är det endast legitimerad personal som har behörighet till NPÖ. Totalt uppgår detta till ca 50 personer inom sektor omsorg. När personal ska tilldelas behörighet används en e-tjänst med digital signering på kommunens intranät. Behörighetstilldelning sker i det som kallas HSA/KOMKAT-katalog och kan göras av systemförvaltare och två assistenter, som är kommunens HSA- och SITHS[1]-handläggare. Behörighetskatalogen administreras av Kommunförbundet Skåne.

I samband med detta sker en avstämning gentemot Socialstyrelsens register över legitimerad personal, vilket säkerställer att personen i fråga har en giltig legitimation. Varje användare får även ett SITHS-kort, som används för tvåfaktorinloggning i systemet.

När den legitimerade personalen avslutar sin anställning ska SITHS-kortet avregistreras och förstöras. En gång per kvartal kontrolleras även SITHS-kort gentemot anställd legitimerad personal.

3.3.2. Loggkontroller

Enligt rutin för åtkomstkontroll i NPÖ genomförs kontroller en gång per kvartal. Systemförvaltaren tar fram en lista med loggar under en månad, varpå ett urval görs av 10 % av antalet patienter som förekommer i listan.

Ansvarig chef ska sedan kontrollera patientrelationen samt att det finns ett registrerat samtycke. Kontrollen dokumenteras i ett granskningsprotokoll som lämnas till systemförvaltaren. Det genomförs ingen kontroll att samtliga granskningsprotokoll har inkommit till systemförvaltaren.

3.3.3. Bedömning

Vi bedömer att kontroll och uppföljning av systemet är ändamålsenligt. Systemet i sig har inbyggda funktioner som möjliggör detta. Dock vill vi återigen lyfta avsaknaden av en systemförvaltningsplan, som enligt kommunens systemförvaltarmodell ska finnas. Samt att det inte kontrolleras att granskningsprotokoll lämnas in efter genomförda loggkontroller.

3.4. Stickprovskontroll av loggar

EY har gjort ett slumpmässigt urval av 15 brukare för Procapita VOO, varpå den medarbetare som visat aktivitet hos brukaren valdes ut för kontrollen. Kontrollen omfattade sedan aktiviteterna under en veckas tid. Ett av urvalen omfattade en medarbetare som avslutat sin tjänst vilket innebar att 14 medarbetare granskades. Totalt efterfrågades kontroller från 11 enhetschefer varav 9[2] återkom. Omfattningen av kontrollen beslutades i samråd med systemförvaltaren.

[1] SITHS e-legitimation används av personer inom vård och omsorg som identifiering med stark autentisering vid inloggning i e-tjänster.
[2] Totalt 8 inom tidsfristen på 14 dagar.

Totalt inkom granskning av 13 medarbetare som haft aktiviteter i Procapita. I de granskningar som genomfördes fann enhetscheferna inga avvikelser.

Ett slumpmässigt urval av 10 brukare gjordes för NPÖ, och därefter valdes den aktuella ut för kontrollen. Kontrollen omfattade aktiviteten under fyra sammanhängande veckor. Totalt inkom granskning av 9 medarbetare. I de granskningar som genomfördes fann enhetscheferna inga avvikelser.

3.4.1. Bedömning

I samband med stickprovet framkom inga avvikelser avseende aktiviteten inne i systemen, vilket vi bedömer vara positivt. Däremot visade stickprovet på svagheter i processen eftersom vissa stickprov inte genomfördes.

4. Sammanfattande bedömning

Vår sammanfattande bedömning är att arbetet med behörigheter, åtkomster och loggkontroller inte fungerar helt ändamålsenligt, därtill bedömer vi att den interna kontrollen inte är fullt ut tillräcklig. Vi bedömer att kommunstyrelsens övergripande styrning inom området bör stärkas och att styrelsen bör förtydliga riktlinjer och rekommendationer kring systemförvaltningen och säkerställa att verksamheterna upprättar adekvat systemdokumentation.

Avseende omsorgsnämnden är det vår bedömning att arbetet med behörigheter, åtkomster och loggkontroller inte fungerar helt ändamålsenligt. Vi bedömer att nämnden behöver stärka styrningen av behörigheter och även stärka den interna kontrollen.

Revisionsfrågor	Svar
Är ansvars- och arbetsfördelningen inom organisationen tillräckligt tydlig?	Delvis. Det finns en fastställd systemförvaltarmodell som beskriver ansvarsfördelning inom organisationen. Dock kan den behöva ses över tillsammans med mallen för systemförvaltarplan. Därutöver bedömer vi att det saknas tydliga riktlinjer för verksamheterna att förhålla sig till när det gäller gallring, åtkomst och loggkontroller.
Är uppföljning och utvärdering inom området ändamålsenlig?	Delvis. Det genomförs återkommande kontroller i båda verksamhetssystem. Dock inte i den utsträckning som framgår av riktlinjer, och enligt vår bedömning är kontrollerna i Procapita inte tillräckligt omfattande.
Sker en tillräcklig styrning av behörigheter till känsliga system?	Delvis. Det finns en tydlig rutin för hur behörigheter ska beställas. Däremot saknas en fastställd behörighetförteckning/villkor för behörigheter.
Säkerställer nämnderna att tillräcklig intern kontroll inom området har upprättats för att hindra otillåten åtkomst till och spridning av känslig information?	Delvis. Stickprovet uppvisade inga avvikelser i aktiviteten. Däremot visade stickprovet på att det finns brister i förfarandet, vilket även påpekats av de intervjuade. En adekvat uppföljning av gjorda loggkontroller görs inte, dvs loggkontroller som inte skickas in till förvaltningen efterfrågas inte heller. Vid stickprovet visade det sig också att samtliga kontroller inte utfördes. Därtill ska verksamhetssystemen ha en fastställd systemförvaltarplan, vilket de granskade systemen inte har. Vi har i granskningen inte kunnat se att det finns någon kontroll av att systemförvaltarplaner upprättas.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Stärka styrningen av arbetet med informationssäkerhet i kommunens verksamhetssystem.

Utifrån granskningsresultatet rekommenderar vi omsorgsnämnden att:

- Stärka styrningen vid behörighetstilldelning.
- Säkerställa att åtkomstkontroller sker i den utsträckning som krävs i fråga om frekvens och omfattning.
- Upprätta systemförvaltarplaner i enlighet med systemförvaltarmodellen.

Kävlinge den 13e maj 2019

Jakob Smith
EY

Emmy Lundblad
EY

Bilaga 1 Källförteckning

Intervjuade funktioner:

- Systemförvaltare (IT-samordnare) för NPÖ och Procapita VOO, kommunikationsenheten
- Medicinskt ansvarig sjuksköterska, sektor omsorg
- IT-strateg,-kommunkansliet

Medverkat vid intervjuerna:

- Fernando Dinis-Viseu, förtroendevald revisor
- Per-Åke Rask, förtroendevald revisor

Dokument:

- Systemförvaltarmodell
- Mall för systemförvaltarplan
- Informationssäkerhet Procapita VOO rutin
- Åtkomstkontroll hälso- och sjukvårdsjournaler för legitimeras personal rutin
- Åtkomstkontroll hälso- och sjukvårdsjournaler samt SoL och LSS-akter vårdpersonal rutin
- Granskningsprotokoll åtkomstkontroll
- Patientsäkerhetsberättelse 2018

Bilaga 2 Forum

Nivå	Benämning	Deltagare	Område
Verksamhetssystem	Användarforum	Systemförvaltare Systemadministratör Superanvändare	Utvecklingsärenden, supportfrågor, rutiner, dokumentation och utbildning.
Verksamhetssystem	Leverantörsforum	Systemförvaltare Driftansvarig Leverantör	Supportärenden, avtal.
Verksamhetssystem	Avtalsuppföljning	Systemägare Systemförvaltare Vid behov: ansvarig för inköp och leverantör	Avtalsefterlevnad, licenser och kostnader.
Förvaltningsgrupp	Utvecklingsråd	Systemägare Systemförvaltare Processägare Vid behov: driftansvarig	Utvecklingsärenden, större förändringar, nya system.
Kommungemensamt	Systemförvaltarforum	Förvaltare av systemförvaltarmodellen Systemförvaltare	Systemförvaltarmodellen, verktyg, gruppdiskussioner och erfarenhetsutbyte.